

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-288939

(43) 公開日 平成8年(1996)11月1日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06			H 0 4 L 9/02	Z
	9/14	7259-5 J	G 0 9 C 1/00	
G 0 9 C 1/00			H 0 4 H 1/02	E
H 0 4 H 1/02				F
			H 0 4 N 7/167	Z

審査請求 未請求 請求項の数 2 O L (全 8 頁) 最終頁に続く

(21) 出願番号 特願平7-90641

(22) 出願日 平成7年(1995)4月17日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 ▲高▼野 裕昭

東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

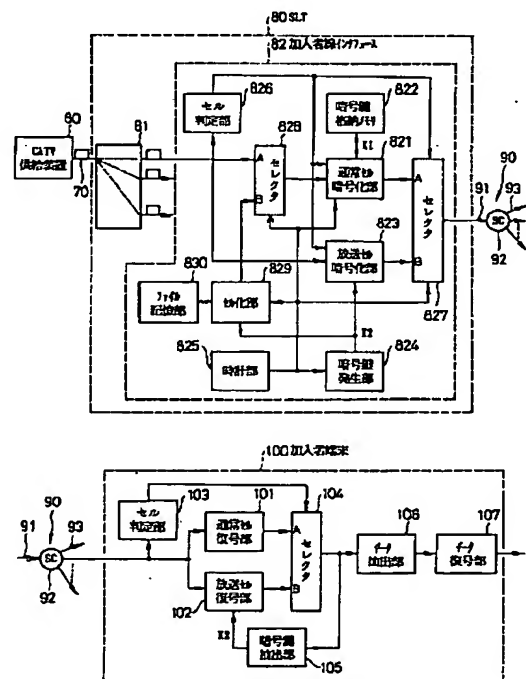
(74) 代理人 弁理士 工藤 宜幸

(54) 【発明の名称】 放送システム

(57) 【要約】

【目的】 時間的な放送スイッチを用いることなく、各加入者線に接続された複数の契約端末にのみ放送サービスを提供することができるようにする。

【構成】 回線終端装置80の放送セル暗号化部823と、暗号鍵発生部824と、時計部824等は、所定の周期で更新される暗号鍵K2を使って、放送セルを暗号化する機能を有する。セル化部829と、ファイル記憶部830と、通常セル暗号化部721等は、暗号鍵K2が更新されるたびに、この暗号鍵K2をセル化し、このセルを各契約者に予め付与された暗号鍵K1で暗号化する機能を有する。加入者端末100の通常セル復号部101は、予め自端末に付与された暗号鍵K1を使って受信セルを復号する機能を有する。暗号鍵抽出部105はこの復号出力から暗号鍵K2を抽出する機能を有する。放送セル復号部102は、この抽出出力を使って受信セルを復号する機能を有する。



一実施例の構成図

【特許請求の範囲】

【請求項 1】 放送情報の送信側に設けられ、この放送情報の送信信号を第 1 の暗号鍵を使って暗号化する第 1 の暗号化手段と、

前記放送情報の送信側に設けられ、前記第 1 の暗号鍵を所定の周期で更新する暗号鍵更新手段と、

前記第 1 の暗号鍵が更新されるたびに、この第 1 の暗号鍵の送信信号を各契約者ごとに予め付与された第 2 の暗号鍵を使って暗号化する第 2 の暗号化手段と、

前記放送情報の受信側に設けられ、受信信号を予め自分に付与された前記第 2 の暗号鍵を使って復号する第 1 の復号手段と、

前記放送情報の受信側に設けられ、前記第 1 の復号手段の復号出力から前記第 1 の暗号鍵を抽出する暗号鍵抽出手段と、

前記放送情報の受信側に設けられ、前記暗号鍵抽出手段の抽出出力を使って前記受信信号を復号する第 2 の復号手段とを具備したことを特徴とする放送システム。

【請求項 2】 前記第 1 の暗号化手段と、前記暗号鍵更新手段と、前記第 2 の暗号化手段は、加入者網の加入者線終端装置に設けられ、

前記第 1 の復号手段と、前記暗号鍵抽出手段と、前記第 2 の復号手段は、加入者線を介して前記加入者線終端装置に接続される加入者端末に設けられていることを特徴とする請求項 1 記載の放送システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、伝送路として、例えば、広帯域サービス総合ディジタル網（以下「B-I S D N」という。）を使って放送を行う放送システムに関する。

【0002】

【従来の技術】近年、電気通信の分野においては、電話網のような加入者網として、B-I S D N の導入が進められている。この B-I S D N においては、通信サービスとして、有線テレビジョン（以下「C A T V」という。）をはじめとする放送型サービスの提供が予想される。このため、例えば、下記の文献等に記載されるように、B-I S D N における放送型サービスの提供に関する研究開発が盛んに行われている。

【0003】文献：「マルチメディアサービスを提供する広帯域アクセス系の検討」

信学技報 TECHNICAL REPORT OF IEICE. CS94-18. OSC94-8(1994-05)

図 2 は、B-I S D N を使った C A T V システムの構成の一例を示すブロック図である。

【0004】図示の C A T V システムにおいては、C A T V 供給装置 10 から出力された C A T V 信号の放送セルは、B-I S D N の中核をなす長距離網 20 を介して加入者線終端装置（S L T）30 に供給される。

【0005】加入者線終端装置 30 に供給された放送セルは、複数の加入者線 40 に振り分けられる。各加入者線 40 に振り分けられた放送セルは、この加入者線 40 に接続された複数の加入者端末（O N U）50 に振り分けられる。

【0006】各加入者線 40 は、例えば、パッシブダブルスター方式の伝送路によって構成されている。すなわち、各加入者線 40 は、加入者線終端装置 30 に接続される 1 本の光ファイバ 41 と、スターカプラ（S C）42 と、各加入者端末 50 に接続される複数の光ファイバ 43 によって構成されている。

【0007】しかしながら、加入者線 40 をパッシブダブルスター方式の伝送路で形成するような構成では、放送サービスの契約者以外の者にも放送サービスが提供されてしまうという問題が生じる。

【0008】すなわち、放送サービスの契約は、通常、放送チャンネルごとに行われる。また、B-I S D N を使った放送サービスの場合、さらに、時間単位の契約が考えられる。言い換えれば、番組単位の契約が考えらる。

【0009】このような契約環境の下では、各加入者線 40 に接続された複数の加入者端末 50 がすべて契約者の加入者端末（以下「契約端末」という。）とは限らない。したがって、加入者線 40 をパッシブダブルスター方式の伝送路で形成するような構成では、放送サービスの契約者以外の者にも放送サービスが提供されてしまうという問題が生じる。

【0010】この問題に対処するために、従来は、加入者線終端装置 30 において、予め各加入者端末 50 に付与された暗号鍵を使って、各契約者ごとに放送セルを暗号化して送信するようになっていた。

【0011】このような構成によれば、各契約端末 50 しか受信セルを復号することができないので、契約者のみ放送サービスを提供することができる。

【0012】

【発明が解決しようとする課題】しかしながら、このような構成では、放送セルの放送スイッチとして、空間的な放送スイッチのほかに、時間的な放送スイッチが必要になるという問題があった。

【0013】ここで、空間的な放送スイッチ 31 とは、図 3 に示すように、C A T V 供給装置 10 から供給される放送セルを複数の出線 32 に振り分けるスイッチである。

【0014】また、時間的な放送スイッチ 33 とは、図 4 に示すように、放送セルを契約端末数分だけ複写し、各複写セルを各出線 32 に時分割で出力することにより、1 つの加入者線 40 に接続されている複数の契約端末 50 に放送セルを振り分けるスイッチである。

【0015】このような時間的な放送スイッチが必要になると、各加入者の使用可能な帯域が狭められてしまうという問題が生じる。

3

【0016】また、図5に示すように、放送スイッチ33の内部に放送セルの複写部34を設ける構成では、放送セルを最大で[出線数] * [出線に接続される加入者端末数]分複写しなければならないため、バッファメモリの負荷が大きくなってしまいう問題が生じる。

【0017】さらに、図6に示すように、放送スイッチ33の出線32上に放送セルの複写部34を設けるような構成では、各出線32ごとにバッファメモリを設けなければならないという問題が生じる。

【0018】したがって、加入者線40として、パッシブダブルスター方式の伝送路を用いる放送システムにおいては、時間的な放送スイッチ33を用いることなく、放送を行うことができるような技術が望まれる。

【0019】

【課題を解決するための手段】上記課題を解決するために、この発明は、放送情報の送信信号を所定の周期で更新される第1の暗号鍵を使って暗号化して送信し、かつ、この第1の暗号鍵が更新されるたびに、この第1の暗号鍵の送信信号を各契約者ごとに予め付与された第2の暗号鍵を使って暗号化して送信するようにしたものである。

【0020】

【作用】上記構成においては、放送情報の送信側では、放送情報の送信信号を第1の暗号鍵で暗号化して送信する処理が実行される。また、第1の暗号鍵が更新されるたびに、この暗号鍵の送信信号を各契約者に予め付与された第2の暗号鍵で暗号化して送信する処理が実行される。

【0021】一方、放送情報の受信側では、予め自分に付与された第2の暗号鍵を使って受信信号を復号する処理が実行される。また、この復号出力から第1の暗号鍵を抽出する処理が実行される。さらに、この抽出出力を使って受信信号を復号する処理が実行される。

【0022】このような構成によれば、受信された第1の暗号鍵の送信信号が予め自分に付与された第2の暗号鍵で暗号化されたものであれば、この受信信号から正確に第1の暗号鍵を抽出することができる。これにより、時間的な放送スイッチを用いることなく、受信された放送情報の送信信号を正確に復号することができる。

【0023】

【実施例】以下、図面を参照しながら、この発明の実施例を詳細に説明する。

【0024】図1は、この発明の一実施例の構成を示すブロック図である。

【0025】なお、図1は、この発明を、B-ISDNを使ったCATVシステムに適用した場合を代表として示す。また、図1は、この発明を、放送セルのほかに通常セルの伝送機能を有するシステムに適用した場合を代表として示す。ここで、通常セルとは、1つの加入者端末100にのみ供給されるATM（非同期転送モード）

4

セルである。

【0026】図示の放送システムは、CATV供給装置60と、長距離網70と、加入者線終端装置80と、複数の加入者線90と、複数の加入者端末100を有する。なお、図には、1つの加入者線90と、1つの加入者端末100を示す。

【0027】ここで、CATV供給装置60は、CATV信号の放送セルを出力する機能を有する。長距離網70は、ATMセル（放送セルや通常セル）を加入者線終端装置80まで伝送する機能を有する。加入者線終端装置80は、加入者線90を終端する機能を有する。加入者線90は、加入者端末100と加入者線終端装置80とを接続する機能を有する。加入者端末100は、CATV信号のATMセルを受信する機能を有する。

【0028】加入者線終端装置80は、放送スイッチ81と、複数の加入者線インタフェース82を有する。

【0029】ここで、放送スイッチ81は、長距離網70を介して送られてきたATMセルを複数の加入者線インタフェース82に分配する機能を有する。図には、1つの加入者線インタフェース82を示す。各加入者線インタフェース82は、放送スイッチ81と加入者線90とを接続する機能を有する。

【0030】各加入者線90は、1つの光ファイバ91と、1つのスターカプラ92と、複数の光ファイバ93からなるパッシブダブルスター方式の伝送路として構成されている。

【0031】ここで、光ファイバ91は、対応する加入者線インタフェース80とスターカプラ92とを接続する機能を有する。光カプラ92は、光ファイバ91から供給されるATMセルを分岐する機能を有する。光ファイバ93は、スターカプラ92と各加入者端末100とを接続する機能を有する。

【0032】加入者線インタフェース82は、通常セル暗号化部821と、暗号鍵格納メモリ822と、放送セル暗号化部823と、暗号鍵発生部824と、時計部825と、セル判定部826と、セクタ827、828と、セル化部829と、ファイル記憶部830を有する。

【0033】ここで、通常セル暗号化部821は、通常セルの宛先の加入者端末100に予め付与された暗号鍵K1を使って、当該通常セルを暗号化する機能を有する。暗号鍵格納メモリ822は、対応する加入者線90に接続された複数の加入者端末100のそれぞれに予め付与された暗号鍵K1を各加入者線100ごとに保持する機能を有する。

【0034】放送セル暗号化部823は、暗号鍵K2を使って、放送セルを暗号化する機能を有する。暗号鍵発生部824は、暗号鍵K2を出力する機能を有する。また、この暗号鍵発生部824は、時計部825から供給される制御信号に基づいて、暗号鍵K2を所定の周期で

更新する機能を有する。時計部 8 2 5 は、暗号鍵 K 2 の更新タイミングを示す制御信号を出力する機能を有する。

【0035】セル判定部 8 2 6 は、放送スイッチ 8 1 から出力される A T M セルが通常セルか放送セルかを判定する機能を有する。

【0036】セクタ 8 2 7 は、セル判定部 8 2 6 により A T M セルが通常セルと判定されると、通常セル暗号化部 8 2 1 の出力を選択し、放送セルと判定されると、放送セル暗号化部 8 2 3 の出力を選択する機能を有する。また、このセクタ 8 2 7 は、暗号鍵 K 2 が変更されると、セル判定部 8 2 6 の判定結果に関係なく、一時的に、通常セル暗号化部 8 2 1 の出力を選択する機能を有する。

【0037】セクタ 8 2 8 は、通常は、放送スイッチ 8 1 から出力される A T M セル（放送セルや通常セル）を選択し、暗号鍵 K 2 が更新されると、一時的に、セル化部 8 3 0 から出力される暗号鍵のセルを選択する機能を有する。この選択出力は、通常セル暗号化部 8 2 1 に供給される。

【0038】セル化部 8 2 9 は、暗号鍵 K 2 の更新時に、この暗号鍵 K 2 をセル化する機能を有する。このセルは通常セルとして形成される。この通常セルを以下暗号鍵セルという。ファイル記憶部 8 3 0 は、加入者の情報ファイル（以下「加入者ファイル」という。）を格納する機能を有する。この加入者ファイルには、加入者に関する各種情報が登録される。

【0039】なお、暗号鍵発生部 8 2 4 は、各放送チャネルごとに暗号鍵 K 2 を発生する。また、放送セル暗号化部 8 2 3 は、受け取った放送セルの放送チャネルを判定し、判定した放送チャネルに対応する暗号鍵 K 2 で当該放送セルを暗号化する。

【0040】加入者端末 1 0 0 は、通常セル復号部 1 0 1 と、放送セル復号部 1 0 2 と、セル判定部 1 0 3 と、セクタ 1 0 4 と、暗号鍵抽出部 1 0 5 と、データ抽出部 1 0 6 と、データ復号部 1 0 7 を有する。

【0041】ここで、通常セル復号部 1 0 1 は、対応する光ファイバ 9 3 を介して送られてきた受信セルを予め自装置に付与された暗号鍵 K 1 を使って復号する機能を有する。同様に、放送セル復号部 1 0 2 は、この受信セルを暗号鍵抽出部 1 0 5 の抽出出力を使って復号する機能を有する。

【0042】セル判定部 1 0 3 は、受信セルが通常セルか放送セルかを判定する機能を有する。セクタ 1 0 4 は、セル判定部 1 0 3 によりセルが通常セルと判定されると、通常セル復号部 1 0 1 の出力を選択し、放送セルと判定されると、放送セル復号部 1 0 2 の出力を選択する機能を有する。暗号鍵抽出部 1 0 5 は、セクタ 1 0 4 の選択出力から暗号鍵 K 2 を抽出する機能を有する。

【0043】データ抽出部 1 0 6 は、セクタ 1 0 4 の

選択出力から A T M セルのペイロード部分に挿入されているデータを抽出する機能を有する。データ復号部 1 0 7 は、データ抽出部 1 0 6 により抽出されたデータを復号する機能を有する。

【0044】上記構成において、動作を説明する。

【0045】まず、放送システム全体の動作を説明する。

【0046】C A T V 供給装置 6 0 から出力された放送セルは、長距離網 7 0 を介して加入者線終端装置 8 0 に供給される。また、この加入者線終端装置 8 0 には、放送セル以外の通常セルも供給される。

【0047】加入者線端末装置 8 0 は、入力セルが通常セルであれば、これを、その宛先に基づいて、複数の加入者線 9 0 のいずれか 1 つに送出する。加入者線 9 0 に送出された通常セルは、この加入者線 9 0 に接続された複数の加入者端末 1 0 0 に供給される。この複数の加入者端末 1 0 0 に供給された通常セルは、その宛先に応じた加入者端末 1 0 0 でのみ正常に復号される。

【0048】これに対し、入力セルが放送セルであれば、これを複数の加入者線 9 0 に振り分ける。各加入者線 9 0 に振り分けられた放送セルは、この加入者線 9 0 に接続された複数の加入者端末 1 0 0 に供給される。この複数の加入者端末 1 0 0 に供給された放送セルは、当該放送チャネルの契約端末 1 0 0 でのみ正常に復号される。以上が、図 1 の放送システムの全体的な動作である。

【0049】次に、加入者線終端装置 8 0 の動作を説明する。

【0050】C A T V 供給装置 6 0 から加入者線終端装置 8 0 に送られてきた放送セルは、まず、放送スイッチ 8 1 に供給される。放送スイッチ 8 1 は、入力セルが通常セルであれば、これを複数の加入者線インタフェース 8 2 のうち、その宛て先に応じた加入者線インタフェース 8 2 に供給する。これに対し、放送セルであれば、複数の加入者線インタフェース 8 2 に供給する。

【0051】この加入者線インタフェース 8 2 の動作は、暗号鍵 K 2 の更新時以外の期間の動作と暗号鍵 K 2 の更新時の動作に大別される。したがって、以下の説明では、この 2 つの場合に分けて、加入者線インタフェース 8 2 の動作を説明する。

【0052】まず、暗号鍵 K 2 の更新時以外の期間の動作を説明する。

【0053】放送スイッチ 8 1 から出力される A T M セル（通常セルや放送セル）は、セクタ 8 2 8 と、放送セル暗号化部 8 2 3 と、セル判定部 8 2 6 に供給される。また、セル化部 8 2 9 から出力される暗号鍵セルは、セクタ 8 2 8 に供給される。

【0054】セクタ 8 2 8 は、暗号鍵 K 2 の更新時以外の期間は、放送スイッチ 8 1 から出力される A T M セルを選択する。これにより、この場合は、通常セル暗号

10

20

30

40

50

化部 8 2 1 には、放送スイッチ 8 1 から出力される A T Mセルが供給される。

【 0 0 5 5 】セル判定部 8 2 6 は、入力セルが通常セルか放送セルかを判定する。この判定結果は、通常セル暗号化部 8 2 1 と、放送セル暗号化部 8 2 3 と、セクタ 8 2 7 に供給される。

【 0 0 5 6 】通常セル暗号化部 8 2 1 は、入力セルが通常セルの場合は、この入力セルの宛先の加入者端末 1 0 0 に予め定められた暗号鍵 K 1 を使って、この入力セルを暗号化する。この暗号鍵 K 1 は、暗号鍵格納メモリ 8 2 2 から読み出される。これに対し、放送セルの場合は、この暗号化処理を中止する。この通常セル暗号化部 8 2 1 の出力は、セクタ 8 2 7 に供給される。

【 0 0 5 7 】放送セル暗号化部 8 2 3 は、入力セルが放送セルの場合は、暗号鍵発生部 8 2 4 から出力される暗号鍵 K 2 を使って、この入力セルを暗号化する。これに対し、通常セルの場合は、この暗号化処理を中止する。この放送セル暗号化部 8 2 3 の出力は、セクタ 8 2 7 に供給される。

【 0 0 5 8 】セクタ 8 2 7 は、セルが通常セルの場合は、通常セル暗号化部 8 2 1 の出力を選択し、放送セルの場合は、放送セル暗号化部 8 2 3 の出力を選択する。これにより、セルが通常セルの場合は、セクタ 8 2 7 から通常セルの暗号化出力が出力され、放送セルの場合は、放送セルの暗号化出力が出力される。

【 0 0 5 9 】この暗号化出力は、加入者線 9 0 を介してこの加入者線 9 0 に接続されるすべての加入者端末 1 0 0 に供給される。以上が、暗号鍵 K 2 の更新時以外の期間の動作である。

【 0 0 6 0 】次に、暗号鍵 K 2 の更新時の動作を説明する。

【 0 0 6 1 】この場合も、放送スイッチ 8 1 から出力される A T Mセルは、セクタ 8 2 8 と、セル判定部 8 2 6 と、放送セル暗号化部 8 2 3 に供給される。また、セル化部 8 2 9 から出力される暗号鍵セルは、セクタ 8 2 8 に供給される。さらに、セル判定部 8 2 6 の判定結果は、通常セル暗号化部 8 2 1 と、放送セル暗号化部 8 2 3 と、セクタ 8 2 7 に供給される。

【 0 0 6 2 】しかし、この場合、セクタ 8 2 8 では、時計部 8 2 5 から出力される制御信号に従って、セル化部 8 2 9 の出力が選択される。また、通常セル暗号化部 8 2 1 では、セル判定部 8 2 6 の判定結果に関係なく、通常セル入力時の動作が行われる。さらに、セクタ 8 2 7 では、セル判定部 8 2 6 の判定結果に関係なく、通常セル暗号化部 8 2 1 の出力が選択される。

【 0 0 6 3 】これにより、この場合は、セル化部 8 2 8 から出力される暗号鍵セルがセクタ 8 2 8 を介して通常セル暗号化部 8 2 1 に供給され、暗号化される。この暗号化出力は、セクタ 8 2 7 を介して加入者線 9 0 に出力され、この加入者線 9 0 に接続された複数の加入者

端末 1 0 0 に供給される。以上が暗号鍵 K 2 の更新時の動作である。

【 0 0 6 4 】ここで、セル化部 8 2 9 の動作を詳細に説明する。

【 0 0 6 5 】このセル化部 8 2 9 では、暗号鍵 K 2 の更新時、まず、暗号鍵発生部 8 2 4 から出力されるある放送チャンネルの暗号鍵 K 2 をセル化する処理が実行される。これにより、暗号鍵セルが得られる。この暗号鍵セルは、通常セルとして形成される。但し、この段階では、その宛先情報（仮想パス識別子や仮想チャンネル識別子等）は挿入されていない。

【 0 0 6 6 】次に、この暗号鍵セルを複写する処理が実行される。この複写は、当該放送チャンネルの契約者数分だけ繰り返される。但し、この場合の契約者数は、対応する加入者線 9 0 に接続されている契約者数である。

【 0 0 6 7 】このとき、同時に、各契約者の宛先情報を挿入する処理も実行される。この宛先情報は、ファイル記憶部 8 3 0 に格納されている加入者ファイルから読み出される。

【 0 0 6 8 】このようにして生成された契約者数分の暗号鍵セルは、順次セクタ 8 2 8 を介して、通常セル暗号化部 8 2 1 に供給される。この後、次の放送チャンネルの暗号鍵 K 2 について、上述したような処理が実行される。以下、同様に、すべての放送チャンネルの暗号鍵 K 2 について、上述した処理が繰り返される。

【 0 0 6 9 】通常セル暗号化部 8 2 1 に供給された暗号鍵セルは、放送スイッチ 8 1 から供給される通常セルと同様に、その宛先に対応する暗号鍵 K 1 を使って暗号化される。以上がセル化部 8 2 9 の動作である。

【 0 0 7 0 】次に、加入者端末 1 0 0 の動作を説明する。

【 0 0 7 1 】光ファイバ 9 3 を介して送られてきた受信セル（通常セル（暗号鍵セルを含む）や放送セル）は、通常セル復号部 1 0 1 と、放送セル復号部 1 0 2 と、セル判定部 1 0 3 に供給される。

【 0 0 7 2 】通常セル復号部 1 0 1 に供給された受信セルは、当該端末に割り当てられた暗号鍵 K 1 を使って復号される。この復号出力は、セクタ 1 0 4 に供給される。また、放送セル復号部 1 0 2 に供給された受信セルは、暗号鍵抽出部 1 0 5 の抽出出力を使って復号される。この復号出力は、セクタ 1 0 4 に供給される。

【 0 0 7 3 】セル判定部 1 0 3 に供給された受信セルは、通常セル（暗号鍵セルを含む）か放送セルかを判定される。この判定結果は、セクタ 1 0 4 に供給される。セクタ 1 0 4 は、受信セルが通常セルの場合は、通常セル復号部 1 0 1 の復号出力を選択し、放送セルの場合は、放送セル復号部 1 0 2 の出力を選択する。

【 0 0 7 4 】これにより、受信セルが通常セルの場合は、通常セル復号部 1 0 1 の復号出力が暗号鍵抽出部 1 0 5 と、データ抽出部 1 0 6 に供給される。これに対

し、放送セルの場合は、放送セル復号部 1 0 2 の復号出力がこれらに供給される。

【0075】暗号鍵抽出部 1 0 5 は、セクタ 1 0 4 の選択出力から暗号鍵 K 2 を抽出する。この抽出出力は、放送セル復号部 1 0 2 に復号用の暗号鍵として供給される。データ抽出部 1 0 6 は、セクタ 1 0 4 の選択出力からペイロードに挿入されているデータを抽出する。但し、この抽出は、入力セルが暗号鍵セルである場合は、中止される。抽出されたデータは、データ復号部 1 0 7 によりデジタル信号からアナログ信号に戻される。

【0076】通常セルの暗号化に用いられた暗号鍵 K 1 が自端末に付与された暗号鍵 K 1 と一致する場合、この通常セルは正確に復号される。これにより、この場合は、この通常セルのペイロードに挿入されているデータが正確に抽出される。その結果、この場合は、この通常セルを使って送られてきた情報が正確に再生されることになる。

【0077】また、この場合、この通常セルが暗号鍵セルであれば、この暗号鍵セルから暗号 K 2 が正確に抽出される。これにより、この場合は、放送セルが正確に復号される。その結果、この場合は、この放送セルのペイロードに挿入されているデータが正確に抽出される。これにより、この場合は、この放送セルを使って送られてきた情報が正確に再生されることになる。

【0078】これに対し、通常セルの暗号化に用いられた暗号鍵 K 1 が自端末に付与された暗号鍵 K 1 と一致しない場合は、この通常セルが正確に復号されない。これにより、この場合は、この通常セルを使って送られてきた情報が正確に再生されないことになる。

【0079】また、この場合は、暗号鍵 K 2 も正確に抽出されないため、放送セルも正確に復号されない。これにより、この場合は、この放送セルを使って送られてきた情報が正確に再生されないことになる。

【0080】以上詳述したこの実施例によれば、次のような効果が得られる。

【0081】(1) まず、この実施例によれば、放送セルを所定の周期で更新される暗号鍵 K 2 を使って暗号化して送信し、かつ、この暗号鍵 K 2 が更新されるたびに、この暗号鍵 K 2 をセル化し、かつ、この暗号鍵セルを各契約者ごとに予め付与された暗号鍵 K 1 を使って暗号化して送信するようにしたので、各加入者線 9 0 に複数の契約端末 1 0 0 が接続されている場合であっても、これらに一度で放送セルを放送することができる。

【0082】これにより、時間的な放送スイッチを用いることなく、各加入者線 9 0 に接続された複数の契約端末 1 0 0 に放送セルを供給することができるので、各加入者の使用帯域が狭められるという問題と、バッファメモリの負荷や量が大きくなるという問題を回避することができる。

【0083】(2) また、この実施例によれば、暗号

鍵 K 2 を所定の周期で更新するようにしたので、契約が番組単位で更新されるような契約においては、暗号鍵 K 2 の更新周期を例えば 5 分単位とすることにより、この暗号鍵 K 2 の更新によって、実質的に契約を解除することができるという利点が得られる。一方、契約が年単位で更新されるような契約においては、暗号鍵 K 2 の更新によって、この暗号鍵 K 2 の秘密性を高めることができるという利点が得られる。

【0084】(3) また、この実施例によれば、暗号鍵 K 2 を契約者に送信する場合、予めすべての暗号鍵 K 2 を送信するのではなく、この暗号鍵 K 2 が更新されるたびに、1 つずつ送るようにしたので、暗号鍵 K 2 として、乱数を用いることができる。これにより、暗号鍵 K 2 の秘密性を高めることができる。

【0085】(4) さらに、この実施例によれば、暗号鍵 K 2 を契約者に送信する場合、この暗号鍵 K 2 をセル化した後、各契約者に付与された暗号鍵 K 1 で暗号化して送信するようにしたので、この暗号鍵 K 2 を通常セルの送信系を使って送信することができる。これにより、暗号鍵 K 2 を送信するために追加するハードウェア量を極力少なくすることができる。

【0086】以上、この発明の一実施例を説明したが、この発明は、上述したような実施例に限定されるものではない。

【0087】(1) 例えば、先の実施例では、この発明を、パッシブダブルスター方式の加入者線 9 0 を使った放送システムに適用する場合を説明した。しかし、この発明は、アクティブダブルスター方式の加入者線を使った放送システムに適用しても構わない。すなわち、契約者を含む複数の加入者に放送を行うシステムだけでなく、契約者のみに放送を行うシステムに適用しても構わない。

【0088】(2) また、先の実施例では、この発明を、セル交換方式のような蓄積交換方式の通信網を使って放送を行う放送システムに適用する場合を説明した。しかし、この発明は、回線交換方式の通信網を使って放送を行う放送システムにも適用することができる。

【0089】(3) また、先の実施例では、この発明を、交換方式の通信網を使って放送を行う放送システムに適用する場合を説明した。しかし、この発明は、交換方式の通信網ではなく、例えば、複数のノードがメッシュ状に接続された通信網を使った放送システムにも適用することができる。

【0090】(4) このほかにも、この発明は、その要旨を逸脱しない範囲で、種々様々変形実施可能なことは勿論である。

【0091】

【発明の効果】以上詳述したようにこの発明によれば、放送情報の送信信号を所定の周期で更新される第 1 の暗号鍵を使って暗号化して送信し、かつ、この暗号鍵が更

新されるたびに、この暗号鍵の送信信号を各契約者ごとに予め付与された第2の暗号鍵を使って暗号化して送信するようにしたので、1つの加入者線に複数の契約端末が接続されている場合であっても、これらに一度で放送情報を放送することができる。

【0092】これにより、時間的な放送スイッチを用いることなく、各加入者線に接続された複数の契約端末に放送情報を供給することができるので、各加入者の使用帯域が狭められるという問題と、バッファメモリの負荷や量が大きくなるという問題を回避することができる。

【図面の簡単な説明】

【図1】この発明の一実施例の構成を示すブロック図である。

【図2】CATVシステムの一例の構成を示すブロック図である。

【図3】空間的放送スイッチの機能を説明するためのブロック図である。

【図4】時間的放送スイッチの機能を説明するためのブロック図である。

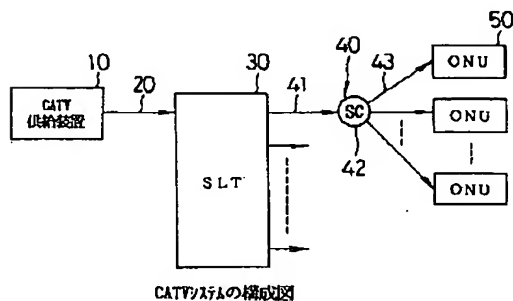
【図5】時間的放送スイッチの構成の一例を示すブロック図である。

【図6】時間的放送スイッチの構成の他の例を示すブロック図である。

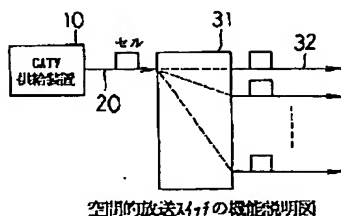
【符号の説明】

- 60…CATV供給装置
- 70…長距離網
- 80…加入者線終端装置
- 90…加入者線
- 100…加入者端末
- 81…放送スイッチ
- 82…加入者線インタフェース
- 91, 93…光ファイバ
- 92…スターコプラ
- 821…通常セル暗号化部
- 822…暗号鍵格納メモリ
- 823…放送セル暗号化部
- 824…暗号鍵発生部
- 825…時計部
- 826, 103…セル判定部
- 827, 828, 104…セクタ
- 829…セル化部
- 830…ファイル記憶部
- 101…通常セル復号部
- 102…放送セル復号部
- 105…暗号鍵抽出部
- 106…データ抽出部
- 107…データ復号部

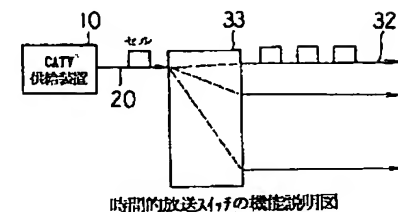
【図2】



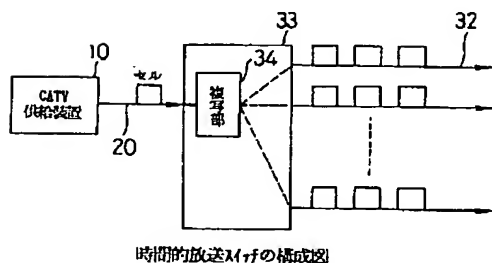
【図3】



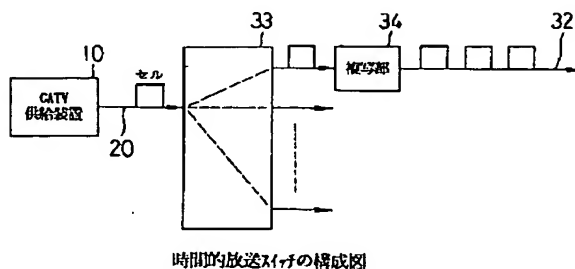
【図4】



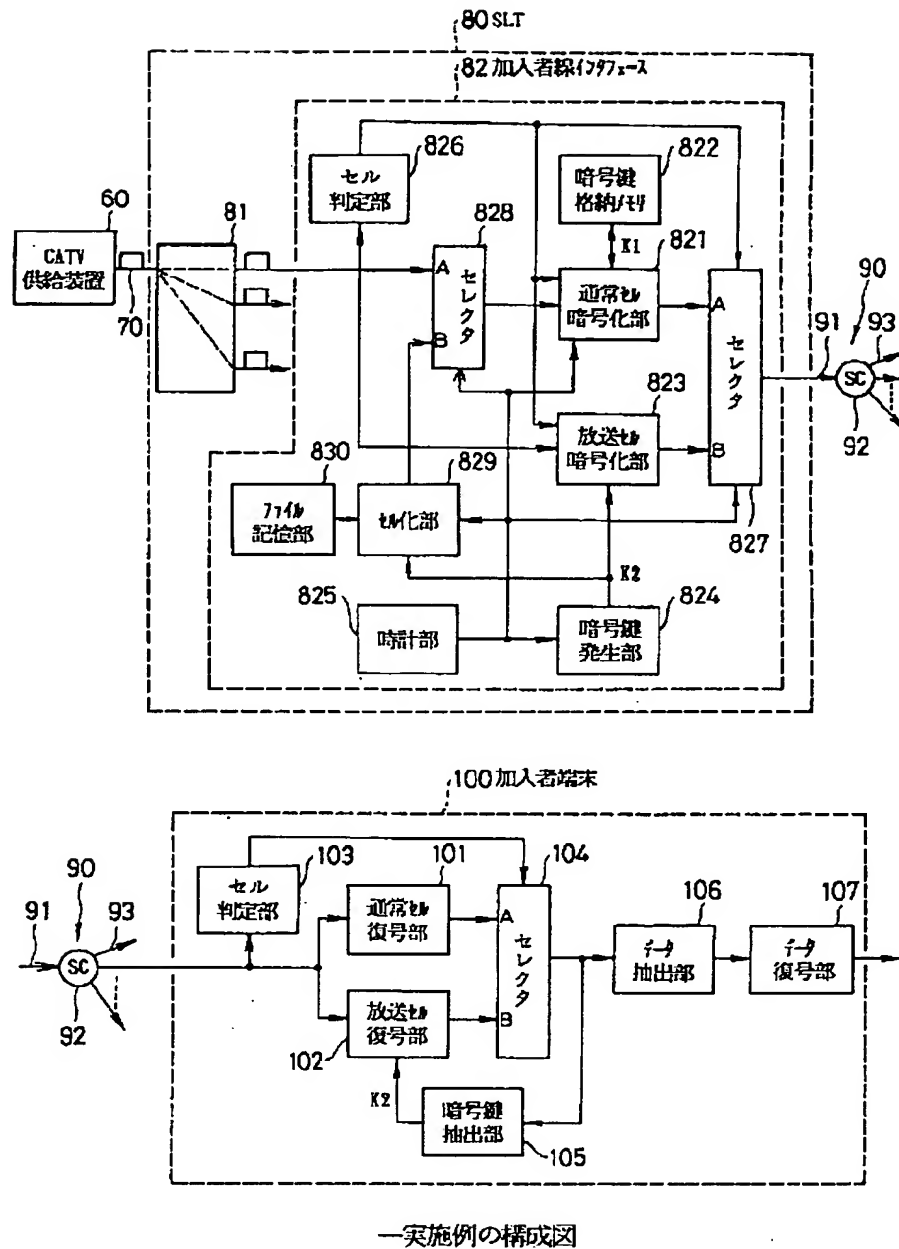
【図5】



【図6】



【図 1】



フロントページの続き

(51) Int. Cl. 6

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 N 7/167